

What is claimed is:

1. A random sequence generating apparatus for generating a sequence of integers of w bits, comprising:

5 a seed receiving section which receives a sequence of integers $s_1, s_2, \dots, s_n, \dots, s_m$ of w bits as a seed for integers n and m ($1 \leq n \leq m-1$);

an initialization section which provides a transformation section with said received sequence of integers $s_1, s_2, \dots, s_n, \dots, s_m$ as an integer sequence $x_1, x_2, \dots, x_n, \dots, x_m$;

10 said transformation section which performs predetermined transformation on each of said provided integer sequence $x_1, x_2, \dots, x_n, \dots, x_m$ to acquire a sequence of integers $y_1, y_2, \dots, y_n, \dots, y_m$ of w bits;

a rotation section which acquires a number of rotation bits from said sequence of integers y_{n+1}, \dots, y_m , performs a rotation operation on said acquired number of rotation bits with respect to all of or a part of said sequence of integers $y_1, y_2, \dots, y_n, \dots, y_m$ taken as a bit sequence of wm bits, and acquires a sequence of integers $z_1, z_2, \dots, z_n, \dots, z_m$ of w bits from

15 said acquired bit sequence of wm bits;

an updating section which provides said transformation section with said sequence of integers $z_1, z_2, \dots, z_n, \dots, z_m$ as said integer sequence $x_1, x_2, \dots, x_n, \dots, x_m$; and

20 an output section which outputs a sequence of integers z_1, z_2, \dots, z_n or z_{n+1}, \dots, z_m obtained last as a random sequence r_1, r_2, \dots, r_n or r_1, \dots, r_{m-n} respectively in case where transformation in said transformation section and rotation in said rotation section are repeated a predetermined number of times.

2. The random sequence generating apparatus according to claim 1, wherein said transformation section performs transformation by recursion formulae given below for an integer i ($1 \leq i \leq m-1$) using mapping $g(\cdot, \cdot)$

25
$$y_1 = g(x_m, x_1)$$

$$y_{i+1} = g(x_i, x_{i+1}).$$

3. The random sequence generating apparatus according to claim 1, wherein said

transformation section performs transformation by recursion formulae given below for an integer i ($1 \leq i \leq m-1$) using a predetermined integer c and mapping $g(\cdot, \cdot)$

$$y_1 = g(c, x_1)$$

$$y_{i+1} = g(y_i, x_{i+1}).$$

- 5 4. The random sequence generating apparatus according to claim 1, wherein said transformation section performs transformation by recursion formulae given below for an integer i ($1 \leq i \leq m-1$) using mapping $g(\cdot, \cdot)$

$$y_1 = g(c, x_1)$$

$$y_{i+1} = g(x_i, x_{i+1}).$$

- 10 5. The random sequence generating apparatus according to claim 2, wherein said mapping $g(\cdot, \cdot)$ is defined as

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

from predetermined mapping $h(\cdot)$ and a predetermined integer q ($0 \leq q \leq 2^{w-1}$).

- 15 6. The random sequence generating apparatus according to claim 5, wherein said mapping $h(\cdot)$ is defined as

$$h(a) = a$$

7. The random sequence generating apparatus according to claim 5, wherein said mapping $h(\cdot)$ is defined by an operation of clearing a predetermined bit in a numerical expression of a given value.

- 20 8. The random sequence generating apparatus according to claim 5, wherein said mapping $h(\cdot)$ is defined by an operation of inverting a predetermined bit in a numerical expression of a given value.

9. The random sequence generating apparatus according to claim 5, wherein said mapping $h(\cdot)$ is defined by an operation of setting 01 to least significant two bits in a numerical expression of a given value.

- 25 10. The random sequence generating apparatus according to claim 1, wherein taking said sequence of integers y_{n+1}, \dots, y_m as a bit sequence of $w(m-n)$ bits, said rotation

...section acquires, as said number of rotation bits, an integer value equivalent to a bit sequence taken as an integer and obtained by arranging at least one bit at a predetermined position extracted from said bit sequence.

5 11. The random sequence generating apparatus according to claim 10, wherein taking said sequence of integers y_{n+1}, \dots, y_m as a bit sequence of $w(m-n)$ bits, said rotation section determines a direction of rotation based on a value of a bit at a predetermined position in said bit sequence.

10 12. The random sequence generating apparatus according to claim 1, wherein said rotation section acquires a number of rotation bits from said sequence of integers y_{n+1}, \dots, y_m , performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers $y_1, y_2, \dots, y_n, \dots, y_m$ taken as a bit sequence of wn bits, acquires a sequence of integers z_1, z_2, \dots, z_n of w bits from said acquired bit sequence of wn bits, performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers y_{n+1}, \dots, y_m taken as a bit sequence of $w(m-n)$ bits, and acquires a
15 sequence of integers z_{n+1}, \dots, z_m of w bits from said acquired bit sequence of $w(m-n)$ bits.

13. An encryption/decryption apparatus comprising:

a random sequence generating section which generates a random sequence r_1, r_2, \dots, r_n by means of a random sequence generating apparatus recited in claim 1;

20 a message receiving section which receives a sequence of integers p_1, p_2, \dots of w bits as a message; and

an encryption/decryption section which outputs a sequence of integers $p_1 \text{ xor } r_1, p_2 \text{ xor } r_2, \dots, p_i \text{ xor } r_{((i+n-1) \bmod n) + 1}$ as a result of encryption or decryption.

14. A random sequence generating method for generating a sequence of integers of w bits, comprising:

25 a seed receiving step which receives a sequence of integers $s_1, s_2, \dots, s_n, \dots, s_m$ of w bits as a seed for integers n and m ($1 \leq n \leq m-1$);

an initialization step which provides a transformation step with said received

sequence of integers $s_1, s_2, \dots, s_n, \dots, s_m$ as an integer sequence $x_1, x_2, \dots, x_n, \dots, x_m$;

said transformation step which performs predetermined transformation on each of said provided integer sequence $x_1, x_2, \dots, x_n, \dots, x_m$ to acquire a sequence of integers $y_1, y_2, \dots, y_n, \dots, y_m$ of w bits;

5 a rotation step which acquires a number of rotation bits from said sequence of integers y_{n+1}, \dots, y_m , performs a rotation operation on said acquired number of rotation bits with respect to all of or a part of said sequence of integers $y_1, y_2, \dots, y_n, \dots, y_m$ taken as a bit sequence of w_m bits, and acquires a sequence of integers $z_1, z_2, \dots, z_n, \dots, z_m$ of w bits from said acquired bit sequence of w_m bits;

10 an updating step which provides said transformation step with said sequence of integers $z_1, z_2, \dots, z_n, \dots, z_m$ as said integer sequence $x_1, x_2, \dots, x_n, \dots, x_m$; and

an output step which outputs a sequence of integers z_1, z_2, \dots, z_n or z_{n+1}, \dots, z_m obtained last as a random sequence r_1, r_2, \dots, r_n or r_1, \dots, r_{m-n} respectively in case where transformation in said transformation step and rotation in said rotation step are repeated a predetermined number of times.

15 15. The random sequence generating method according to claim 14, wherein said transformation step performs transformation by recursion formulae given below for an integer i ($1 \leq i \leq m-1$) using mapping $g(\cdot, \cdot)$

$$y_1 = g(x_m, x_1)$$

20 $y_{i+1} = g(x_i, x_{i+1}).$

16. The random sequence generating method according to claim 14, wherein said transformation step performs transformation by recursion formulae given below for an integer i ($1 \leq i \leq m-1$) using a predetermined integer c and mapping $g(\cdot, \cdot)$

$$y_1 = g(c, x_1)$$

25 $y_{i+1} = g(y_i, x_{i+1}).$

17. The random sequence generating method according to claim 14, wherein said transformation step performs transformation by recursion formulae given below for an

integer i ($1 \leq i \leq m-1$) using mapping $g(\cdot, \cdot)$

$$y_1 = g(c, x_1)$$

$$y_{i+1} = g(x_i, x_{i+1}).$$

18. The random sequence generating method according to claim 15, wherein said
5 mapping $g(\cdot, \cdot)$ is defined as

$$g(a, b) = 2b^2 + h(a)b + q \pmod{2^w}$$

from predetermined mapping $h(\cdot)$ and a predetermined integer q ($0 \leq q \leq 2^{w-1}$).

19. The random sequence generating method according to claim 18, wherein said
mapping $h(\cdot)$ is defined as

10
$$h(a) = a.$$

20. The random sequence generating method according to claim 18, wherein said
mapping $h(\cdot)$ is defined by an operation of clearing a predetermined bit in a numerical
expression of a given value.

21. The random sequence generating method according to claim 18, wherein said
15 mapping $h(\cdot)$ is defined by an operation of inverting a predetermined bit in a numerical
expression of a given value.

22. The random sequence generating method according to claim 18, wherein said
mapping $h(\cdot)$ is defined by an operation of setting 01 to least significant two bits in a
numerical expression of a given value.

20 23. The random sequence generating method according to claim 14, wherein
taking said sequence of integers y_{n+1}, \dots, y_m as a bit sequence of $w(m-n)$ bits, said rotation
step acquires, as said number of rotation bits, an integer value equivalent to a bit sequence
taken as an integer and obtained by arranging at least one bit at a predetermined position
extracted from said bit sequence.

25 24. The random sequence generating method according to claim 23, wherein
taking said sequence of integers y_{n+1}, \dots, y_m as a bit sequence of $w(m-n)$ bits, said rotation
step determines a direction of rotation based on a value of a bit at a predetermined position

in said bit sequence.

25. The random sequence generating method according to claim 14, wherein said rotation step acquires a number of rotation bits from said sequence of integers y_{n+1}, \dots, y_m , performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers $y_1, y_2, \dots, y_n, \dots, y_m$ taken as a bit sequence of wn bits, acquires a sequence of integers z_1, z_2, \dots, z_n of w bits from said acquired bit sequence of wn bits, performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers y_{n+1}, \dots, y_m taken as a bit sequence of $w(m-n)$ bits, and acquires a sequence of integers z_{n+1}, \dots, z_m of w bits from said acquired bit sequence of $w(m-n)$ bits.

26. An encryption/decryption method comprising:
a random sequence generating step which generates a random sequence r_1, r_2, \dots, r_n by means of a random sequence generating apparatus recited in claim 14;
a message receiving step which receives a sequence of integers p_1, p_2, \dots of w bits as a message; and
an encryption/decryption step which outputs a sequence of integers $p_1 \text{ xor } r_1, p_2 \text{ xor } r_2, \dots, p_i \text{ xor } r_{((i+n-1) \bmod n) + 1}$ as a result of encryption or decryption.

27. A program which allows a computer to function as a random sequence generating apparatus as recited in claim 1.

28. A program which allows a computer to function as an encryption/decryption apparatus as recited in claim 13.